REPORT DOCUMENTATION PAGE

Form Approved

OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
11-08-2015	Final	6 May 14 to 5 May 15

4. TITLE AND SUBTITLE

Establishing Information Security Systems via Optical Imaging

5a. CONTRACT NUMBER
FA2386-14-1-4031

5b. GRANT NUMBER
Grant 14IOA076_144031

5c. PROGRAM ELEMENT NUMBER
61102F

6. AUTHOR(S)

Prof. Tat Soon Yeo

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

National University of Singapore
4 Engineering Drive 3
Singapore 117583
Singapore

8. PERFORMING ORGANIZATION REPORT NUMBER

N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

AOARD
UNIT 45002
APO AP 96338-5002

10. SPONSOR/MONITOR'S ACRONYM(S)

AFRL/AFOSR/IOA(AOARD)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
14IOA076_144031

12. DISTRIBUTION/AVAILABILITY STATEMENT

Distribution Code A: Approved for public release, distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The research goal is to establish information security systems via optical imaging, the primary objective is to develop optical imaging technologies to encrypt and authenticate information for data/images storage and transmission, including optical systems for secured information.

15. SUBJECT TERMS

Optical Imaging, Optical Cryptosystems , Diffractive Imaging, Optical Encryption

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Seng Hong, Ph.D.
U	U	U	SAR	17	**19b. TELEPHONE NUMBER** *(Include area code)* +81 42 511 2000

Standard Form 298 (Rev. 8/98)
Prescribed by ANSI Std. Z39.18

AOARD Grant 144031

PIs: Tat Soon Yeo and Xudong Chen

National University of Singapore,
Department of Electrical and Computer Engineering,
4 Engineering Drive 3, Singapore 117583, Singapore

Project: Establishing Information Security Systems via Optical Imaging

Period of performance reported: 05/06 /2014 - 05/05/2015

1. Summary of the Project

In implementing this research project, several research topics as follows have been conducted:

(1) Optical imaging principles, such as interference and diffraction, have been used for designing information encoding methods, and high complexity of the optical technologies has been achieved to design effective and powerful encoding methods for securing information.

(2) In the developed optical-imaging-based security systems, the higher security than electronic cryptography has been achieved. Complementary techniques, such as steganography and compression, have been investigated and integrated into the developed optical information security systems.

(3) Optical information authentication methods have been developed to verify the decoded data/images. —Blind" authentication has been developed for verifying the decrypted data/images, when the direct observation of decrypted data is not possible. Statistical and correlation algorithms, such as spectral-power-modulated nonlinear correlation, have been correspondingly developed for the designed optical-imaging-based security systems.

Research works have been published as journal or conferences papers. In total, **3 journal papers** have been published, **and 3 conference papers** have been presented. In addition, we have been invited to give **2 talks** related to optical security.

2. Details of the Research Work

With the rapid development of modern technologies, information can be easily modified or stolen through various channels, such as internet and cameras. If confidential or important information is not protected, there would be a great threat to a company or even a nation. Hence, information security becomes a great concern for many industry and government sectors (such as military sector), and it is highly necessary to adopt feasible and effective strategies to protect important or confidential information. The research in this project focuses on **establishing information security systems via optical imaging** — highly desirable for a diversity of applications (such as military sector). The main objective is to develop optical imaging technologies to **encrypt and authenticate information for data/images storage and transmission**, and the

developed optical systems can **open up a new and promising research perspective for securing information. In the implementation period, we have made some important contributions, and the technical details are given as follows:**

(2.1) In the first contribution, we have proposed a new method for security-enhanced phase encryption assisted by nonlinear optical correlation via sparse phase, **see the setup in Fig. 1**. Optical configurations are established based on phase retrieval algorithm for encoding the input image and hiding the secret data into phase-only masks. The results illustrate that when one or few phase-only masks generated during the hiding of secret data are sparse, it is possible to integrate these sparse masks into those phase-only masks generated during the encoding of input image. Hence, synthesized phase-only masks are used for the subsequent recovery, and sparse distributions (i.e., binary maps) are correspondingly generated as additional parameters for the retrieval of secret data. It is difficult for unauthorized receivers to know that a small number of useful phase points have been sparsely distributed in the finally-generated phase-only masks for the retrieval of secret data. In practical applications, a large number of differently-encoded masks (generated by encoding different input images and differently secret-data) can be available for enhancing data security. Only when the secret data are correctly extracted and verified, the corresponding input image obtained with valid keys and the identified phase-only masks can be claimed as targeted information. The multiple-layer configuration, i.e., verification of secret data and recovery of correct input image, has also been established for phase-only optical system.

As illustrated in **Fig. 1(a)**, the sender can choose to generate a large number of differently-encoded masks in phase-only optical system, however only one encoded datum (or one pair) can be used for extracting the correct and effective input image during the recovery. Since a huge number of differently-encoded masks can be sent out through communication channels (such as internet), this strategy can effectively confuse the unauthorized receivers and enhance the designed optical security system. However, the problem is how authorized receiver can identify the correct information (i.e., masks) from these numerous materials.

In this contribution, we propose a strategy by optically hiding the secret data into sparse phase for the verification. Phase-only optical system is taken as an example for illustrating the proposed method, however it may be straightforward to apply the proposed method for other optical security systems. **Figure 1(b)** shows a schematic setup for the proposed phase-only optical system. In addition to the input image, additionally secret-data have also been embedded based on the proposed optical system. One phase-only mask generated during the encoding of the input image is also used for the generation of phase-only mask M3 during the hiding of secret data.

To illustrate the iterative process, relationships between the number of iterations and CC (correlation coefficient) values are shown in **Figs. 2(a) and 2(b)** for input-image encoding and secret-data hiding, respectively. The threshold (i.e., a CC value) is set as 0.985, and 5 and 30 iterations are sufficient to find the convergence solutions as shown in **Figs. 2(a) and 2(b)**, respectively. It is also illustrated in **Figs. 2(a) and 2(b)** that a rapid convergence rate can be achieved in the phase retrieval algorithm. The synthesized phase-only mask $\bar{M}_1(x,y)$ can be obtained by compressing mask M3 followed by the substitution over the originally extracted phase-only mask $M_1(x,y)$. Hence, only phase-only masks $\bar{M}_1(x,y)$ and $M_2(\mu,\nu)$ are used for the subsequent recovery, and **Figs. 3(a) and 3(b)** show the finally-generated phase-only masks $\bar{M}_1(x,y)$ and $M_2(\mu,\nu)$, respectively. When the phase-only mask M3 $[M_3(x,y)]$ is compressed,

one sparse distribution, i.e., binary map $K(x,y)$, is correspondingly generated as additional parameter for the recovery of secret data. **Figure 3(c)** shows the parameter $K(x,y)$ which should be applied to correctly extract sparse phase during the decoding of secret data.

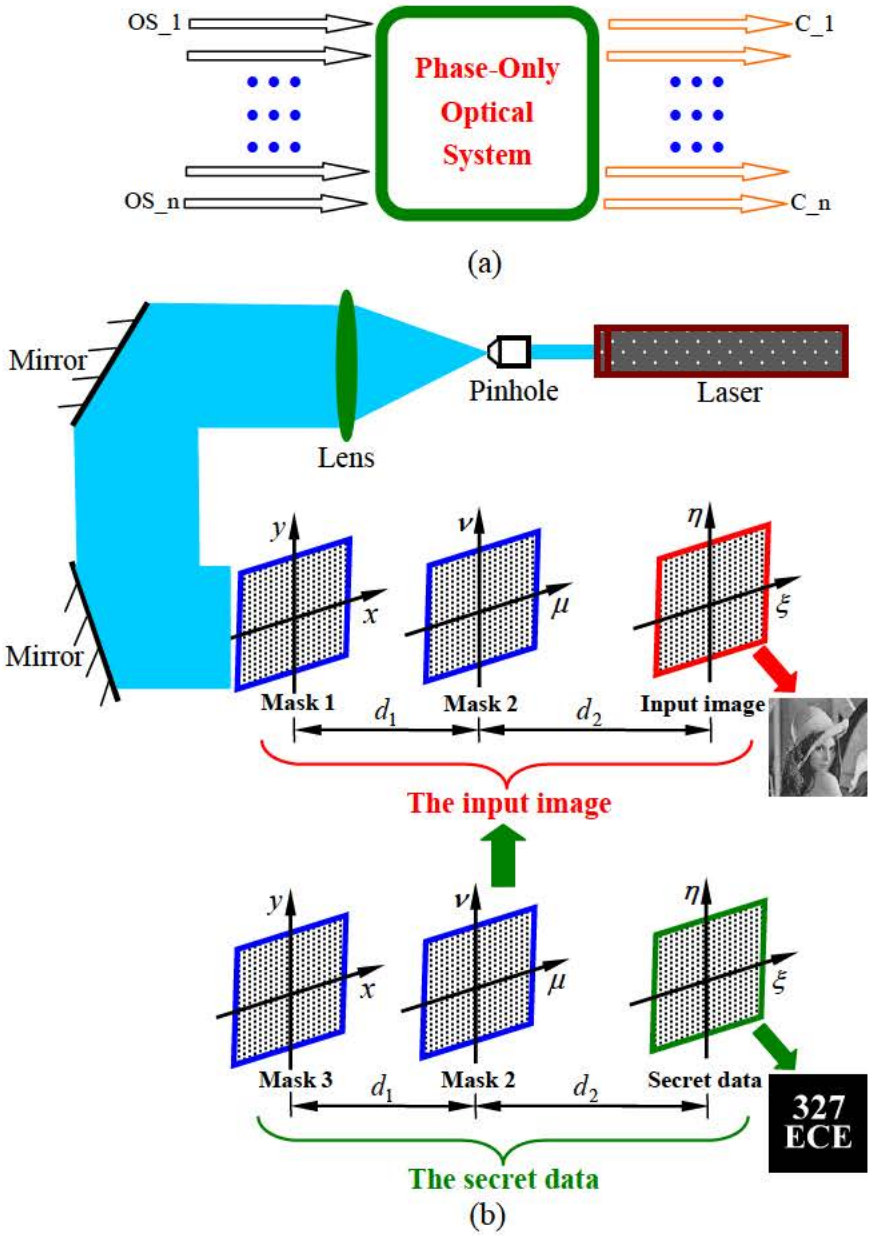


Fig. 1. (a) Schematic for encoding a large number of different optical signals/data through the designed optical system: OS, optical signals/data; C, generated masks (here the series of different phase-only masks generated by the proposed method). (b) A schematic setup for the proposed phase-only optical system: d_1 and d_2 denote axial distances. M1 and M2 are generated during input-image encoding, and M3 is generated during the hiding of secret data. A grayscale image (8 bits), i.e., "Lena", is used as the input image. The binary data containing characters "327 ECE" are used as secret data.

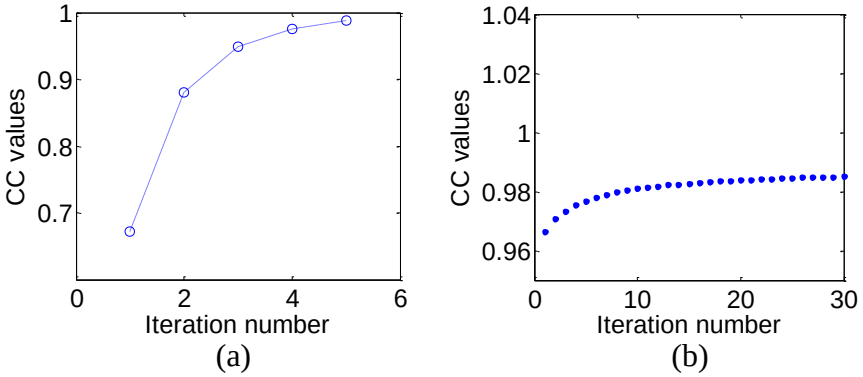


Fig. 2. (a) A relationship between the number of iterations and CC values during the encoding of input image, and (b) a relationship between the number of iterations and CC values during the hiding of secret data.

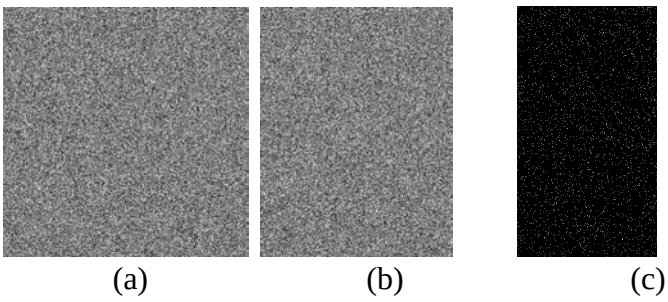


Fig. 3. (a) The finally-generated phase-only mask $\bar{M}_1(x,y)$, (b) the phase-only mask $M_2(\mu,\nu)$, and (c) the sparse map $K(x,y)$, i.e., a binary map.

When the keys are correctly applied during the recovery, the input image and the hidden data can be respectively extracted as shown in **Figs. 4(a) and 4(d)**, respectively. The CCs for **Figs. 4(a) and 4(d)** are 0.7515 and 0.0668, respectively. It can be seen in **Fig. 4(a)** that with correct keys (such as wavelength and distances), the input image can be recovered by using the complete pair of finally-generated phase-only masks $\bar{M}_1(x,y)$ and $M_2(\mu,\nu)$. Although reconstruction quality is affected due to the loss of some phase points (i.e., in mask M1), the recovered image in **Fig. 4(a)** can clearly render the information related to input image. It is worth noting that setup parameters, such as wavelength and axial distances, should be considered as keys for the recovery of the input image. When these parameters are wrong during the recovery, no information about the input image can be obtained as shown in **Figs. 4(b) and 4(c)**. In this contribution, the objective is to illustrate that with acceptable decrease of reconstruction quality (i.e., the input image), much higher security can be achieved in phase-only optical system. Since only a small number of pixels in mask $\bar{M}_1(x,y)$ are useful for the recovery of secret data, the retrieved data as shown in **Fig. 4(d)** cannot clearly render the related information. Nonlinear correlation algorithm is further applied to verify this decoded secret data, and **Fig. 4(e)** shows the nonlinear correlation distribution corresponding to **Fig. 4(d)**. It can be seen in **Fig. 4(e)** that when correct parameters are used for data recovery, the extracted secret data are effectively verified. Only when these retrieved data are effectively authenticated, the reconstructed image in **Fig. 4(a)**

obtained by using valid keys and the identified phase-only masks can be claimed as targeted information. This approach can enhance system security, since multiple-layer configuration is established. More differently secret-data can be further hidden based on the proposed optical system, and one sparse map (i.e., a binary map) can be given to each particular receiver for information verification. In practical applications, when a large number of differently-encoded masks (i.e., only one pair of phase-only masks is authentic and others are counterfeit) are available, the hidden secret data should be first extracted and verified for the identification of correct phase-only masks.

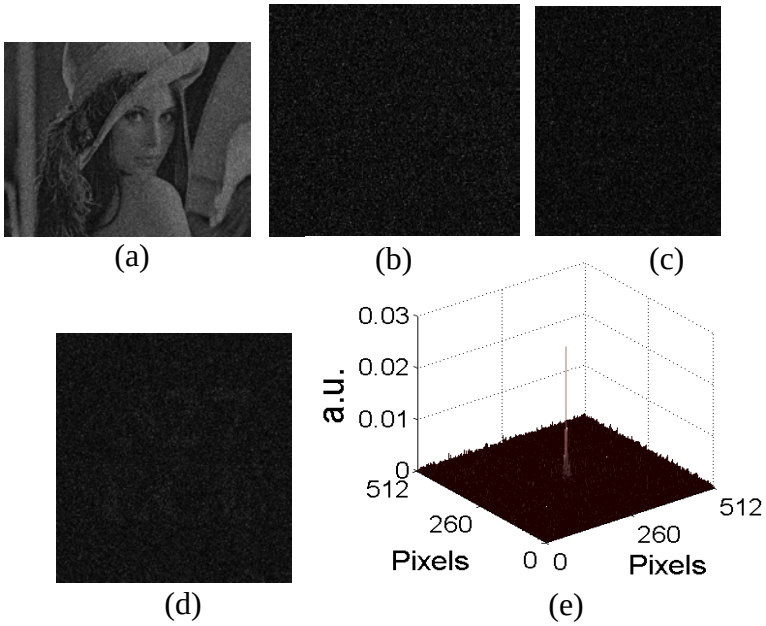


Fig. 4. (a) The recovered input image using correct keys (such as wavelength and distances), the recovered input images using (b) only the wrong wavelength (an error of 10.0 nm) and (c) only the wrong distance d_1 (an error of 1.0 mm), (d) the extracted secret data, and (e) the generated nonlinear correlation distribution corresponding to (d). The CC values for (b) and (c) are -0.0023 and 0.00026, respectively.

(2.2) In the second contribution, we demonstrate that sparsity-based phase-shifting digital holography can be applied for image authentication. In phase-shifting digital holography, the holograms are sequentially recorded. Only small parts of each hologram are available for numerical reconstruction, and nonlinear correlation algorithm can be further applied to simply authenticate the recovered image. It is found that in the developed holographic system, the recorded holograms are highly compressed which can facilitate data storage or transmission, and one simple authentication strategy is established instead of relatively complex algorithms (such as compressive sensing) to recover the object. **Figure 5** shows a schematic setup for the proposed method. The intensity pattern (i.e., a hologram) is recorded by CCD camera via interference between reference and object beams.

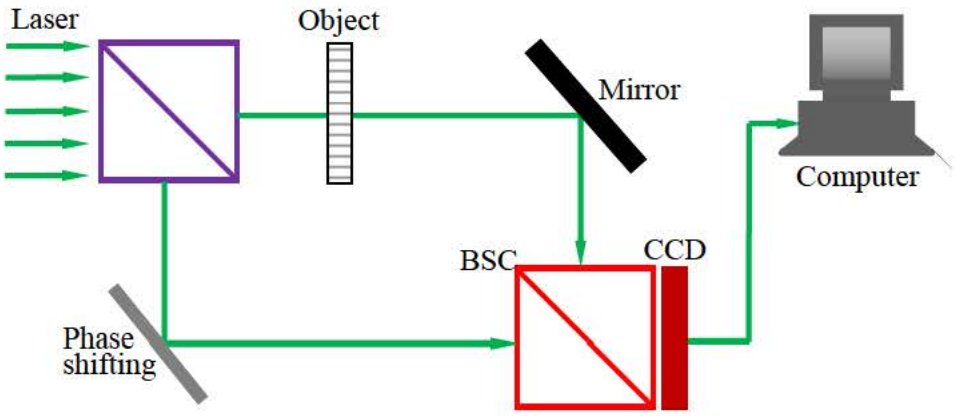
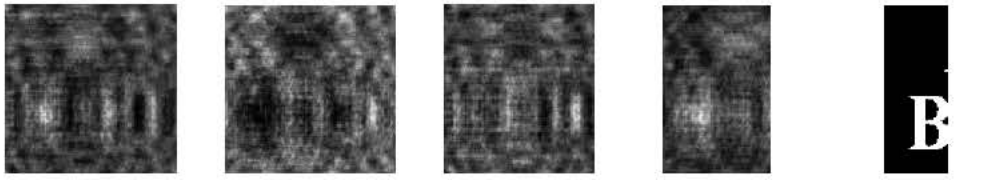


Fig. 5. A schematic setup for the proposed method using holography: BSC, Beam splitter cube; CCD, Charge-coupled device.

The setup shown in **Fig. 5** is conducted to illustrate the feasibility and effectiveness of the proposed method. In our study, pixel size of the CCD camera is $4.65\,\mu m$, and pixel number is 128×128. The collimated plane wave (wavelength of 550 nm) is first generated for the illumination, and axial distance between the object plane and the CCD plane is 35 mm. **Figures 6(a)–6(d)** show four digital holograms, when phase shifting is set as 0, $\pi/2$, π and $3\pi/2$, respectively. **Figure 6(e)** shows a reconstructed object (image), when the recorded holograms are directly applied during the reconstruction. It can be seen in **Fig. 6(e)** that high-quality image can be recovered accordingly. In this case, the complete holograms have been directly applied for object reconstruction.

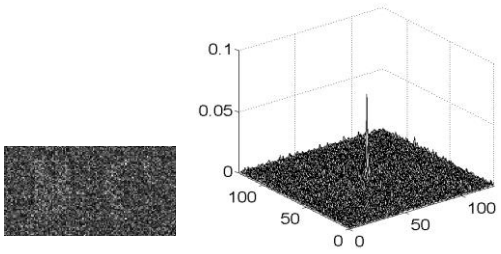


(a) (b) (c) (d) (e)

Fig. 6. Four holograms $[I_i(x,y)\ i=1,2,3,4]$ obtained when phase shifting is set as (a) 0, (b) $\pi/2$, (c) π and (d) $3\pi/2$, respectively. (e) The reconstructed object.

In this contribution, the objective is to apply the sparsity-based phase-shifting digital holography for image authentication, and the recorded holograms are highly compressed. **Figure 7(a)** shows the reconstructed object, when only 5.0% parts of each hologram (pixels randomly selected) are used during numerical reconstruction. It can be seen in **Fig. 7(a)** that the recovered object cannot visually render the information, and is noisy. Nonlinear correlation algorithm is further employed to authenticate the recovered noise-like image, and **Fig. 7(b)** shows the corresponding authentication result. It can be seen in **Fig. 7(b)** that the recovered image is effectively authenticated, since one sharp peak is generated at the center of the correlation distribution. In this contribution, the sparsity-based authentication method is developed for enriching the application domain of holographic technology. The higher sparsifying level could be feasible in sparsity-based authentication system compared with compressive-sensing-based holography. Especially when high sparsifying level (such as 2.0%) is applied, the proposed method

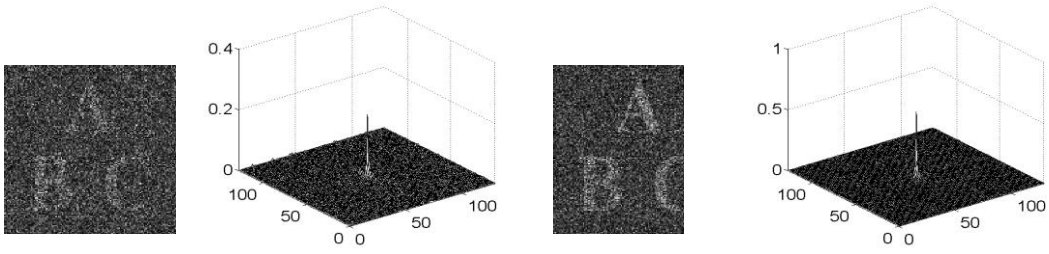
may provide a simple alternative for optical information processing, i.e., simply authenticating the recovered object in holographic system.



(a) (b)

Fig. 7. (a) The reconstructed object obtained when only 5.0% parts of each hologram are used during numerical reconstruction, and (b) the corresponding authentication result (units of horizontal and vertical axes are ~~"~~pixels" and ~~"~~a.u.", respectively).

When more hologram information is used, sharper peaks can be correspondingly generated. However, the reconstructed object could visually render some information about the test object. **Figure 8(a)** shows the reconstructed object, when only 10.0% parts of each hologram (pixels randomly selected) are used during numerical reconstruction. **Figure 8(b)** shows the corresponding authentication result. **Figure 8(c)** shows the reconstructed object, when only 15.0% parts of each hologram (pixels randomly selected) are used during numerical reconstruction. **Figure 8(d)** shows the corresponding authentication result. It is illustrated that in the developed holographic system, the recorded holograms can be highly compressed which will facilitate data storage or transmission, and one simple authentication strategy is established instead of applying relatively complex algorithms (such as compressive sensing) to recover the object. In some applications the recorded holograms may be affected by turbulence media or others (such as noise and occlusion), or the holograms may be damaged in some cases. Hence, these holograms may not be complete for clearly recovering the high-quality object. The proposed method can provide a simple alternative through authenticating the reconstructed object, and a new strategy has been established for holography-based optical signal processing.



(a) (b) (c) (d)

Fig. 8. (a) The reconstructed object obtained when only 10.0% parts of each hologram are used during numerical reconstruction, and (b) the corresponding authentication result. (c) The reconstructed object obtained when only 15.0% parts of each hologram are used during numerical reconstruction, and (d) the corresponding authentication result.

(2.3) In the third contribution, we report how only one random phase-only mask should be pre-generated to be transmitted for ghost-secured imaging system, **see setup in Fig. 9**. During the encoding, a method, called pixel modulation **(see Fig. 10)**, is developed and applied to sequentially modulate the pre-generated random phase-only mask. The proposed method with pixel modulation strategy possesses high security. In addition, only one random phase-only mask and sparsely binary maps (related to positions of selected pixels) are transmitted as principal security keys, hence potential problem (i.e., storage or transmission of a large number of random phase-only masks) in conventional optical security systems can be effectively mitigated to some extent.

Figure 9 shows a schematic of ghost-imaging-based optical security system. In computational ghost imaging, reference intensity patterns can be virtually computed by using phase-only masks (act as keys) without physical recordings, and a series of intensity points, acting as ciphertexts, are recorded at the object beam arm by single-pixel bucket detector (without spatial resolution). In conventional approach, a large number of random phase-only masks should be transmitted for the decoding, hence it is always concerned that data storage or transmission may be tedious.

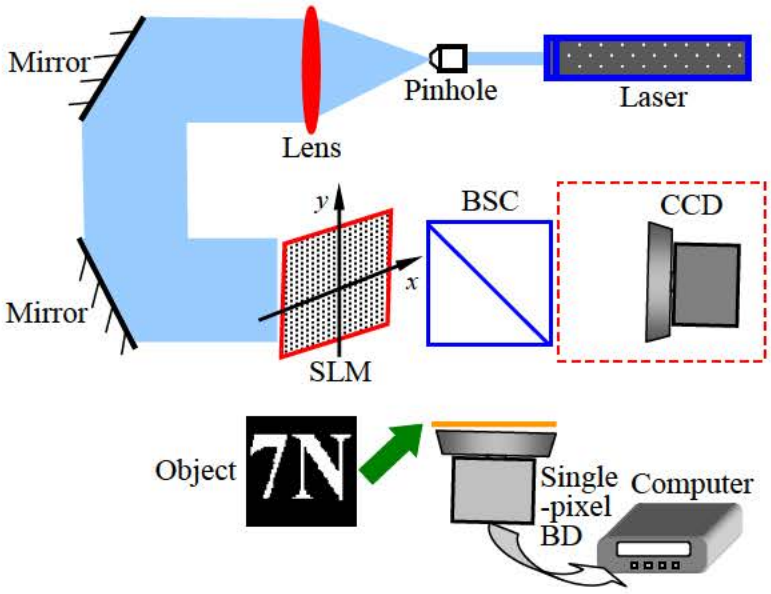


Fig. 9. A schematic for computational ghost imaging: BD, bucket detector; SLM, spatial light modulator; BSC, non-polarizing beam splitter cube; CCD, charge-coupled device. In computational ghost imaging, a series of reference intensity patterns at the reference beam arm can be virtually calculated by using phase-only masks (act as keys), and CCD camera is not requested in this case (indicated by dashed box). Axial distance between SLM and CCD (or BD) is 10.0 cm.

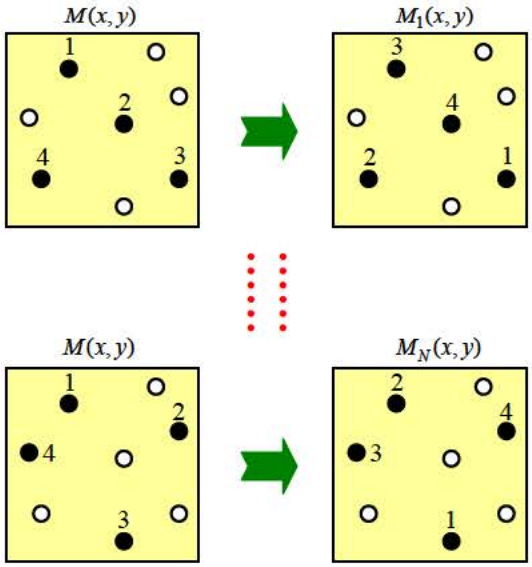


Fig. 10. A schematic of pixel modulation strategy. Non-selected pixels (hollow circles) are maintained, and positions of selected pixels (solid circles) are randomly exchanged (the values of selected pixels are not modified). In this case, 50.0% pixels of phase-only mask $M(x,y)$ are selected for the illustration of the proposed method.

Figure 11(a) shows a recovered object using correct keys, when 10.0% pixels of the originally pre-generated phase-only mask $M(x,y)$ are randomly selected and modulated to generate each phase-only mask [i.e., $M_1(x,y)\ldots\ldots M_N(x,y)$]. The peak signal-to-noise ratio (PSNR) for **Fig. 11(a)** is 9.50 dB. It can be seen in **Fig. 11(a)** that the object can be clearly extracted during the decoding. In the proposed ghost-imaging-based optical security system, the number of selected pixels can be flexibly designed during the encoding. **Figure 11(b)** shows a recovered object using correct keys, when 50.0% pixels of the originally pre-generated phase-only mask $M(x,y)$ are randomly selected and modulated for the generation of each phase-only mask. **Figure 11(c)** shows a recovered object using correct keys, when 90.0% pixels of the originally pre-generated phase-only mask $M(x,y)$ are randomly selected and modulated for the generation of each phase-only mask. The PSNRs for **Figs. 11(b) and 11(c)** are 10.90 dB and 12.13 dB, respectively. The flexible design on the number of selected pixels plays an important role in the developed ghost-imaging-based optical security system, which can guarantee system security.

Figure 12 shows a relationship between the number of selected pixels and quality of recovered objects (PSNR). It can be seen in **Fig. 12** that the higher PSNR can be obtained, when more pixels of the originally pre-generated phase-only mask $M(x,y)$ are randomly selected and modulated for generating a series of phase-only masks. When more pixels are selected and modulated, mutual correlation among the generated phase-only masks [i.e., $M_1(x,y)\ldots\ldots M_N(x,y)$] is lower. Hence, the higher-quality object can be recovered, which satisfies the characteristics (such as speckle-correlation and statistics) of ghost imaging. Since a large range is available for the developed pixel-

modulation strategy, a huge key space can be obtained for the proposed optical security system. In practice, mixed percentages may also be applied to further enhance system security. For instance, the different number of pixels can be randomly selected from pre-generated phase-only mask $M(x,y)$, hence the series of phase-only masks [i.e., $M_1(x,y) \ldots\ldots M_N(x,y)$] is obtained by the modulation of a different number of selected pixels. It is worth noting that it is also possible to directly modulate the whole phase-only mask $M(x,y)$, however random selection of some pixels from $M(x,y)$ followed by pixel modulation can provide the higher security and higher flexibility to the proposed optical security system. As seen in **Fig. 12**, it is also found that when the number of selected pixels is sufficiently large (such as 80.0%), the recovered objects are always of high quality and in this case more selected pixels do not highly lead to quality improvements.

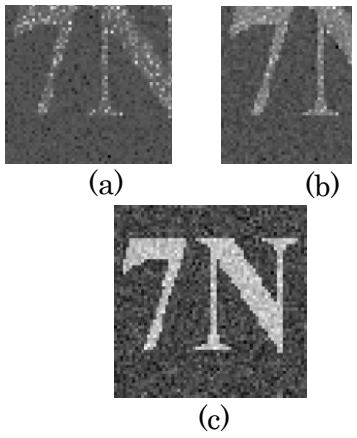


Fig. 11. Correct keys: the recovered objects obtained when (a) 10.0% pixels, (b) 50.0% pixels and (c) 90.0% pixels of the originally pre-generated phase-only mask $M(x,y)$ are randomly selected and modulated to generate each phase-only mask [i.e., $M_1(x,y) \ldots\ldots M_N(x,y)$].

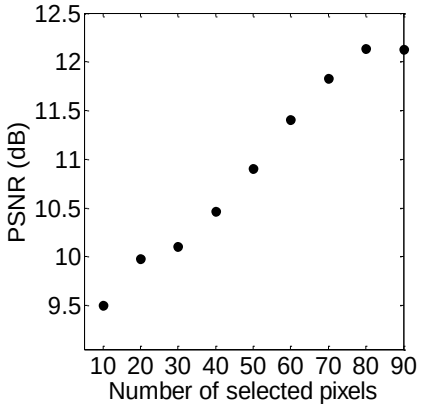


Fig. 12. A relationship between the number of selected pixels (percentage, %) and quality of recovered object (dB). In each encoding and decoding, the pixels are selected from the originally pre-generated phase-only mask $M(x,y)$ to generate each phase-only mask [i.e., $M_1(x,y) \ldots\ldots M_N(x,y)$].

In the proposed ghost-secured imaging system, setup parameters, the originally pre-generated phase-only mask $M(x,y)$, sparsely binary maps (related to positions of selected pixels) and pixel modulation strategy can be considered as security keys. Performance of system keys is further analyzed. **Figure 13(a)** shows a recovered object, when only sparsely binary maps are incorrectly applied during the decoding. The PSNR for **Fig. 13(a)** is 6.86 dB. It can be seen in **Fig. 13(a)** that when the key is wrong during the decoding, no information related to the object can be observed. **Figure 13(b)** shows a recovered object, when the originally pre-generated phase-only mask $M(x,y)$ is wrongly used during the decoding. In this case, pixel modulation is incorrectly applied during object decoding by the unauthorized receivers. The PSNR for **Fig. 13(b)** is 6.83 dB. **Figure 13(c)** shows a recovered object, when only setup parameters are wrong (wavelength error of 10.0 nm and distance error of 0.5 cm) during the decoding. The PSNR for **Fig. 13(c)** is 7.58 dB. All these decoding results illustrate that the keys should be correctly applied for extracting the clear object, and high security is guaranteed in the proposed ghost-imaging-based optical security system. Since only some pixels are randomly selected from $M(x,y)$ during each modulation to generate a series of phase-only masks [i.e., $M_1(x,y)$ …… $M_N(x,y)$], the proposed strategy possesses the higher security than previous method. When simple approaches with translation of a phase-only mask are directly applied for optical encryption, high security may not be effectively guaranteed since translation amounts can be easily estimated via iterative search by the attackers.

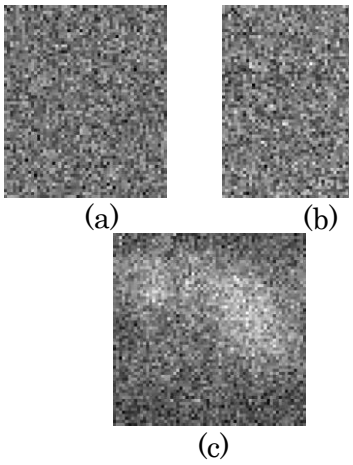


Fig. 13. Wrong keys: the recovered objects obtained (a) when only the sparsely binary maps are incorrectly applied during the decoding, (b) when the originally pre-generated phase-only mask $M(x,y)$ is wrongly used during the decoding, and (c) when only setup parameters are wrong (wavelength error of 10.0 nm and distance error of 0.5 cm) during the decoding. 90.0% pixels of the originally pre-generated phase-only mask $M(x,y)$ are randomly selected and modulated for generating each phase-only mask [i.e., $M_1(x,y)$ …… $M_N(x,y)$].

(2.4) In the fourth contribution, we propose a new method applied to binary image encryption by using a predesigned aperture-key and dual wavelengths. There is no holographic technique needed in the encryption process and the encrypted image is a noise-like intensity image. The security of system is greatly improved in two ways: increasing the key space and disarranging the direct corresponding relation between the output image and the primary image. The aperture key not only helps to mitigate stagnation problems in binary image retrieval, but also enhances the level of security. All decryption keys can be kept in digital form which is convenient for data transmission and digital image retrieval.

An optical setup for the proposed lensless double-random-phase-encoding-based encryption system is schematically shown in **Fig. 14,** where two different chaotic random phase masks are placed at different planes and a CCD camera is placed at the output plane. The original binary data $f(x,y)$ are illuminated by a wavelength-tunable coherent light source and are then encrypted with two pseudorandom phase codes $p_1(x,y)$ and $p_2(x',y')$.

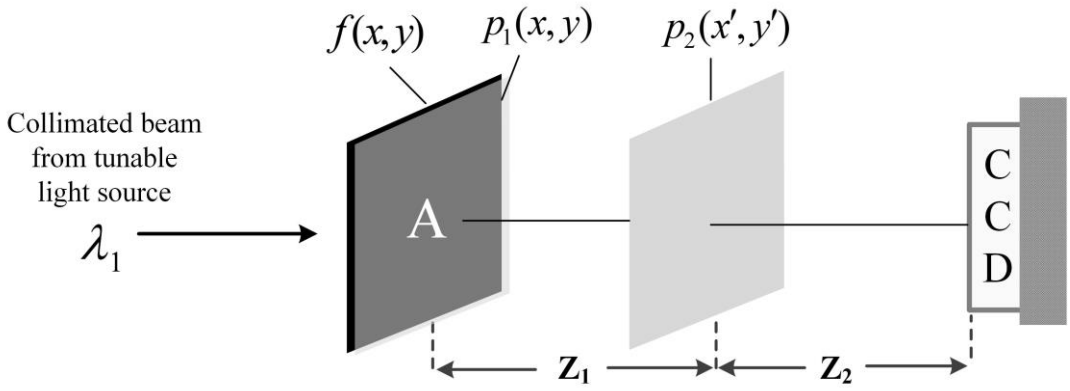


Fig. 14. A schematic optical setup for binary image encryption without holographic recording.

The setup is conducted to show the validity of the proposed method. **Figure 15(a)** shows the test data with the size of 512×512 for a demonstration of the new method. One of the chaotic random phase masks is presented in **Fig. 15(b)**. The CCD camera has 512×512 pixels and $4.6\mu m$ pixel size. **Figure 15(c)** shows the predesigned aperture-key containing all the non-zero regions of the binary image with the smallest possible area. The coded diffraction pattern, i.e., cyphertext, is shown in **Fig. 15(d)**, where the scaling factor is set as $\alpha=3$.

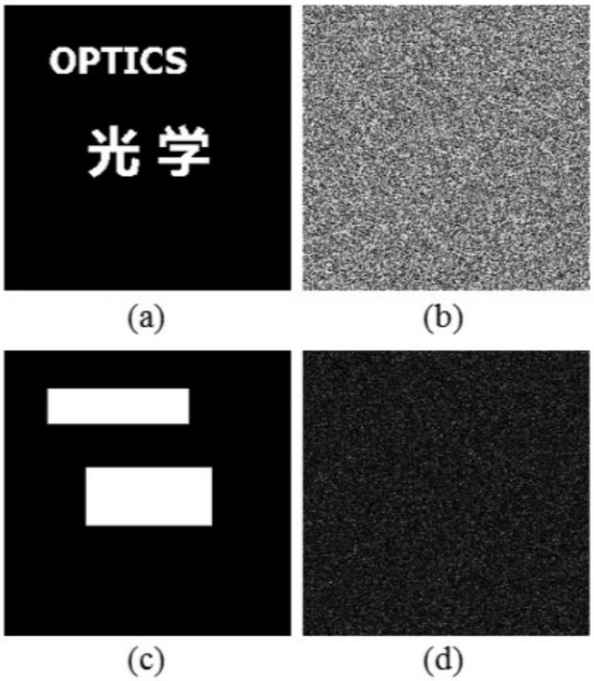


Fig. 15. (a) Plaintext, (b) one of the four CRPMs, (c) aperture key and (d) cyphertext.

We generate a series of cyphertexts by using different scaling factors and then apply the proposed phase retrieve process where all scaling factors are set as $\alpha = 0$ during the decryption. Mean square error (MSE) and correlation coefficient (CC) are used to evaluate the closeness between the primary image and the recovered results by using phase retrieval algorithm, where small deviations in β and γ have no obvious effect on the recovered results. Dependence of MSE on the change of the scaling factor is illustrated in **Fig. 16,** where the sampling interval is chosen as $\Delta\alpha = 0.2$.

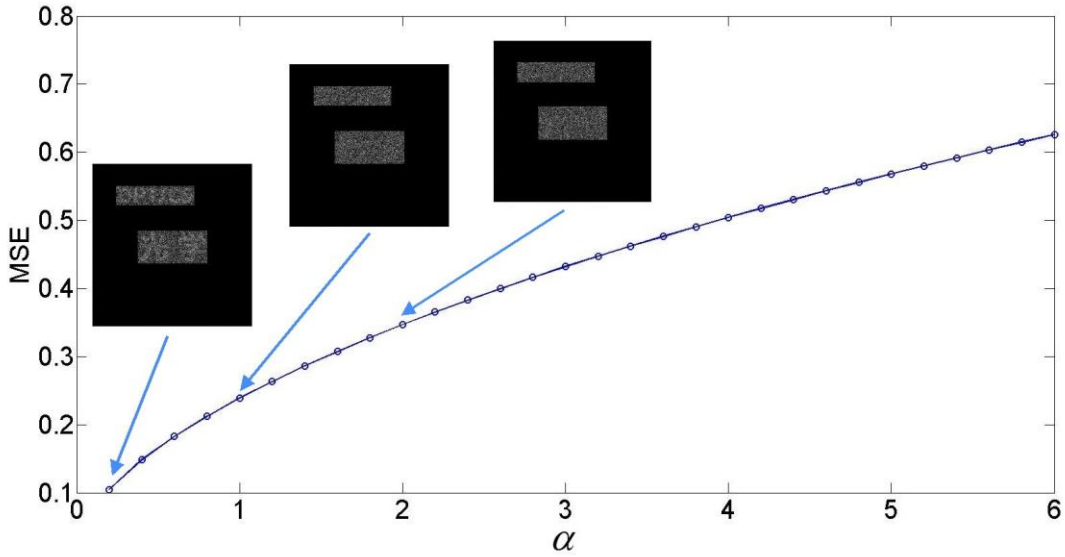


Fig. 16. The MSE curve of recovered images with the changes of scaling factor used for the encryption. The attached three images arranged from left to right correspond to the scaling factor 0.2, 1.0 and 2.0, respectively.

It is found that the MSE value increases as the scaling factor rises. The decrypted

images arranged from left to right in **Fig. 16** correspond to the three scaling factors used for encrypting, i.e., $\alpha = 0.2, \alpha = 1.0$ and $\alpha = 2.0,$ respectively. The recovered images are unrecognizable when the scaling factors are larger than 1. We use all correct keys to recover the primary image from **Fig. 15(d)** with the proposed algorithm. The MSE and CC curves obtained after 50 iterations are respectively presented in **Figs. 17(a) and 17(b).** The CC value reaches its maximum 1 after the number of iterations 31. The finally retrieved image after 50 iterations is depicted by **Fig. 18(a)**. **Figures 17(c) and 17(d)** show MSE and CC curves obtained by conventional GS-based phase retrieval algorithm. It is found that, with the absence of aperture key, convergence speed of phase retrieval algorithm is slow. MSE and CC values corresponding to the number of iterations 1000 are 0.1641 and 0.4777, respectively. The finally recovered image after 1000 iterations is shown in **Fig. 18(b)**.

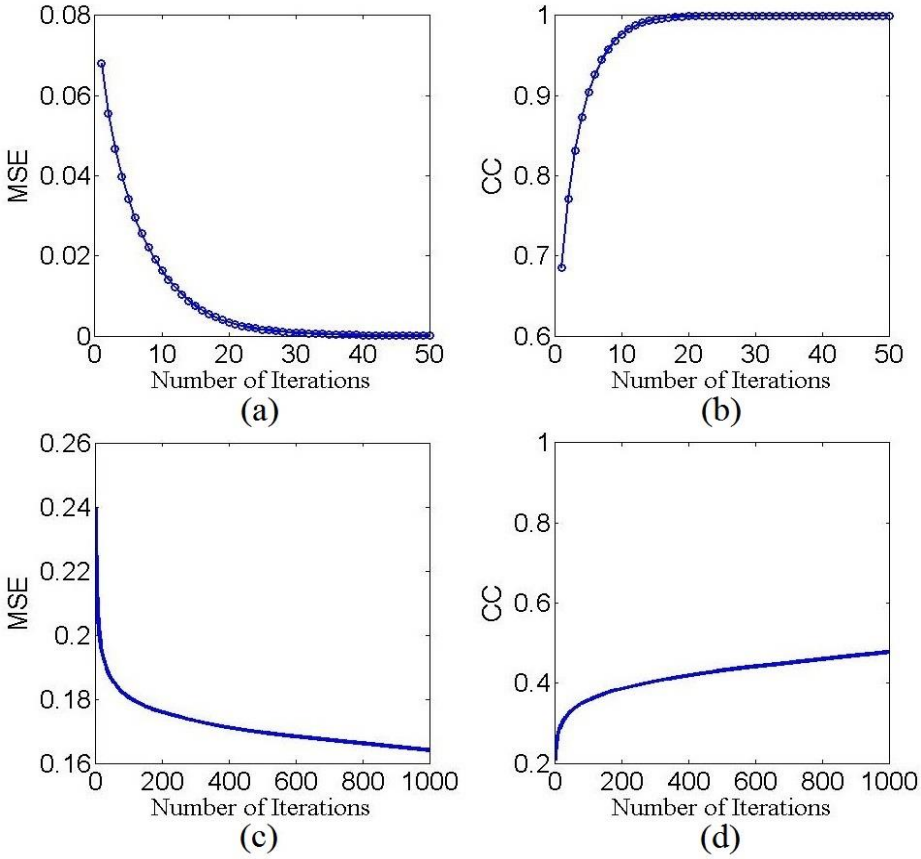


Fig. 17. (a) MSE and (b) CC curves obtained by the proposed method. (c) MSE and (d) CC curves obtained by conventional GS-based phase retrieval algorithm.

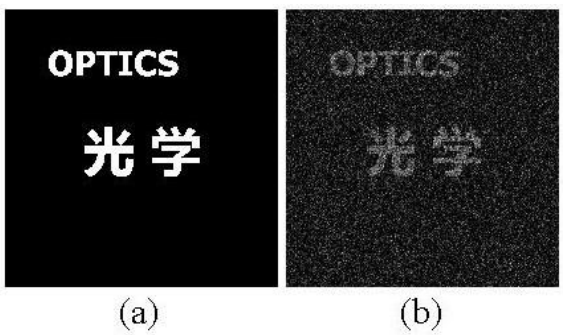


Fig. 18. Retrieved image after (a) 50 iterations using the proposed method, (b) 1000 iterations using conventional GS-based phase retrieval algorithm.

3. Impact of the Research Work

This research project focuses on **establishing information security systems via optical imaging** — highly desirable for a diversity of applications (such as military sector). The main objective is to develop optical imaging technologies to **encrypt and authenticate information for data/images storage and transmission**, and the developed optical systems can **open up a new and promising research perspective for securing information**. Encryption based on optical imaging can attract much attention in many application fields due to its inherent nature of optical signal processing, i.e., parallel processing, high speed, high security, high flexibility and multi-dimensional capabilities. Our research results can be interesting to **many sectors, such as defence sector, domestic security sector and immigration control sector.**

The significance and impact of this research work are briefly summarized as follows:

(a) Optical instruments have parallel-processing and high-speed capabilities. In addition to software platform, optical hardware provides an effective alternative in practical applications.

(b) Higher security has been achieved in the optical encryption systems. Information or materials can be encrypted or hidden in multiple dimensions, such as phase, intensity and light polarization.

(c) Since the sophisticated optoelectronic devices and systems should be analyzed before the retrieval, any hostile hacker will need to possess multi-disciplinary scientific background (such as optics, mathematics, computer, and information theory) and conduct a laborious process of decoding the information (whether in the form of data or images). In other words, before an attacker can even begin a laborious process of decoding, he/she has to gain access to the sophisticated optoelectronic principles and systems where he/she needs to process the information. However, in the military applications, most military information requires **timeliness especially during the war or military conflict**, and the decoded information (**such as commands**) will become invalid to the attacker after a long decoding period.

(d) Various optical principles and configurations have been **investigated**, and a number of powerful optical encoding and authentication methods are developed for securing information. In the developed optical systems, **either digital (virtual optics) or optical approach** can be implemented which can enhance flexibility and applicability of the proposed optical encryption and authentication methods.

(e) In the proposed optical security systems, **encryption capacity** is enhanced to meet the requirement of the receiver/sender, and a number of data/images can be simultaneously compressed and encoded in the optical systems (such as based on phase retrieval).

(f) **Attack approaches** to a designed optical security system can be quantitatively analyzed, and **reliable and effective security-enhancement approach** can be correspondingly implemented for a particularly designed optical-imaging-based security system.

New information security systems are established by using optical imaging. We can choose different optical security options for specific data/images (or called documents), and a hierarchical structure has been designed and optimized for securing information which may have different security levels. There will be **a long-term benefit** that we can use effective and powerful optical-imaging-based systems for encrypting and authenticating information, and various new and updated optical-encryption

methods can still be continuously developed and integrated in the long-term study. **Our proposed methods can provide new and powerful alternatives for protecting military information in defense sector, such as Air Force/DoD.**

Publications:

Journal Papers

[1] Wen Chen, Xiaogang Wang, and Xudong Chen, —Security-enhanced phase encryption assisted by nonlinear optical correlation via sparse phase," Journal of Optics (IOP Publishing), 17, 035702 (12pp), 2015.

[2] Xiaogang Wang, Wen Chen, and Xudong Chen, —Optical binary image encryption using aperture-key and dual wavelengths," Optics Express, vol. 22, 28077–28085, 2014.

[3] Xiaogang Wang, Wen Chen, and Xudong Chen, —Optical image hiding using double-phase retrieval algorithm based on nonlinear cryptosystem under vortex beam illumination," Journal of Optics (IOP Publishing), 17, 035704 (6pp), 2015.

Conference Papers

[4] Wen Chen and Xudong Chen, —Single-pixel optical imaging with compressed reference intensity patterns," SPIE conference, International Conference on Experimental Mechanics (icEM2014) 15–17 Nov. 2014, Singapore.

[5] Wen Chen and Xudong Chen, —Image authentication via sparsity-based phase-shifting digital holography," SPIE conference, 6th International Conference on Graphic and Image Processing (ICGIP 2014), Oct. 24–26, 2014, Beijing, China.

[6] Wen Chen and Xudong Chen, "Ghost-secured imaging via pixel modulation of one phase-only mask," International Conference on Optical and Photonic Engineering, April 14–16 2015, Singapore.

Invited Talks

[7] Our team member was invited by School of Optical and Electronic Information in Huazhong University of Science and Technology (HUST), WuHan City, China, to present an invited talk called —Information Secured by Optics," in 2014 East Lake International Forum for Outstanding Overseas Young Scholars, Dec. 28th–30th, 2014.

[8] Our team member was invited by the organization committee of "International Symposium on 3D Imaging, Metrology, and Data Security" to present a topic of "Optical information encryption and authentication based on ghost imaging" in September 26th–29th, 2015 at Shenzhen, China.